Data Security Policy

1. IT Security

We safeguard the personal information you send to us and all the personal information which we process in the Guild with certain physical, electronic, and managerial procedures within the Guild and within our systems. The Guild's central IT infrastructure is managed by the University of Birmingham, and subject to related policies and procedures.

We also store your and others' personal information behind our firewall and utilise appropriate security measures in our physical facilities to prevent loss or unauthorised use of personal and special information. We limit access to personal information in electronic databases to those persons, including Guild of Students employees, who have a need for such access.

For employees, workers, consultants or volunteers who are issued with a Guild of Students' IT account and email address you will be subject to the Guild's IT & Communications policy and regularly required to update your password. We have measures in place which ensure that you change your password often, use 'strong' passwords that include a combination of letters and numbers, and use a secure browser.

While we do not anticipate breaches in security, if one occurs, we will use all reasonable efforts to correct the problems that led to the breach and we will report it to the Information Commissioner as required under data protection law, and those directly affected.

The Guild's of Students internal IT network and infrastructure is supported and delivered by the University of Birmingham's, IT Services. As such, the Guild complies with University policy in relation to Data and Information Security.

In relation to this the following policies apply and are adopted by the Guild of Students:

- Information Security Policy of the University of Birmingham

Students at the University of Birmingham are also reminded to refer to the: 'General Conditions of Use – University Computer & Network Facilities' which apply to all members of the University of Birmingham.

2. Guidelines for employees, workers, consultants & volunteers *– to be used in conjunction with the Data Protection Policy for Employees, Workers and Consultants and the Volunteer Handbook)*

a. Guidelines for handling personal data – overview

Guild of Students' employees, workers, consultants and volunteers are required to comply with the following guidelines in relation to data which is held or processed on individuals.

A. Employees, workers, consultants and volunteers must ensure that they comply with the Data Protection principles set out in the Guild of Students Student Privacy Policy, and ensure that all records held are:

- processed fairly, lawfully and transparently;
- collected and processed only for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- not kept for longer than is necessary for the purposes for which it is processed; and
- processed securely.

B. Guild employees, workers, consultants and volunteers are responsible for ensuring that any personal data, which they hold, is kept securely, for example:
    - In a locked draw or cabinet;
    - If electronic is password protected;
    - Kept only on an IT services issued disk or devise which is secured/encrypted.

C. Individual employees, workers, consultants and volunteers are responsible for the data which they hold;

D. Individual employees, workers, consultants and volunteers are responsible for ensuring that paper and manual records are destroyed securely using confidential waste bags;

E. Individual employees, workers, consultants and volunteers are responsible for ensuring they comply with the *Data Protection Policy for Employees, Workers and Consultants and the Volunteer Handbook* and that electronic data is stored and disposed of securely;

F. Data should not be disclosed, under any circumstances, without express consent from the Data Protection Officer or CEO or in line with Guild Policy as set out in the Guild Student Privacy Policy or the Guild *Data Protection Policy for Employees, Workers and Consultants*. Unauthorised disclosure of personal data or information in most cases will constitute a disciplinary matter. Please refer to the Staff Code of Conduct for further information.

G. Employees, workers, consultants and volunteers who are responsible for processing personal data should inform the Data Protection Officer or Data Protection Working Group prior to the commencement of any data processing. The Guild of Students may be required to update or amend its Information Commissioner Registration as a result. Questions in relation to this can be directed to the Data Protection Officer or Data Protection Working Group.

H. Employees, workers, consultants and volunteers are responsible for recognising a subject access request (made by an individual with regards to personal data), and treating it appropriately. A subject access request is still valid even if it is not sent to those staff responsible for processing it. Within the Guild, subject access requests are facilitated by the HR & Administration Manager and Data Protection Officer (Director of Operations).

I. All data collected in the course of your work at the Guild, remains the property of the Guild of Students and cannot be used for personal or any other purposes. Failure to comply with this requirement could lead to disciplinary proceedings.

J. Employees, workers, consultants and volunteers must comply with this policy and the Data Protection Act 2018 and the EU General Data Protection Regulation ('GDPR') including when using data outside of the Guild premises. This includes 'taking work home'.

Before any data is processed employees, workers, consultants and volunteers should consult the following checklist:

Guild of Students' checklist for processing data	**Yes/No**
Do you really need to obtain, record and store the information?	
Is the information 'special'?	
If it is special do you have express consent to hold the data from the individual to whom it relates? If not, is one of the other statutory conditions for processing special personal data met? (If in doubt then you must seek the advice of the Data Protection Officer (Director of Operations))	
Has the individual or data subject been informed that the type of data you are collecting will be processed?	
Are you authorized to collect/store/process data?	
If yes, have you checked with the data subject that the data is accurate and up-to-date?	
Is the data you are holding secure?	
Have you notified the Data Protection Working Group/Data Protection Officer that you plan to hold data?	
How long do you need to retain the data, has the data subject been informed, is the privacy notice up to date and do you have a disposal method in place?	

b. Disposal of Data

Employees, workers, consultants and volunteers are responsible for ensuring that data to be disposed of is done so in such a manner as not to compromise the confidentiality of the data. The Facilities Department provide 'Confidential Waste Bags' and arrange for collection and suitable disposal (through incineration) of paper records. This service can be arranged by contacting the Facilities Department. Employees, workers, consultants and volunteers are also responsible for making sure that 'Confidential Waste Bags' are kept secure. If they are open then they should be kept in a locked cupboard or locked room.

The Guild of Students also has an 'Archive & Retention Policy' for the management of records and data.

c. PC Security

Your IT account is provided for your use only, for the purpose of carrying out your job or voluntary role. You must not in any circumstances disclose your password to anyone or allow anyone to access your account or Guild systems using your password/s. If you suspect someone knows your password, you must change it immediately. Disclosing your password is a disciplinary offence under the Guild disciplinary procedure. It is important to keep your password confidential to ensure data security. This helps ensure data you have access to is secure. If you believe your password has been compromised you must change immediately, or contact the IT department. Similarly all employees, workers, consultants and volunteers must lock their computers when they are away from their desk to prevent unauthorised access.

d. Storing IT Data on the Guild Network

It is important that all files relating to your department are stored in an appropriate place on the network. Usually, this will be the departmental folder on the N or O drive accessible through 'My Computer'. Personal files should be stored in your 'My Documents' folder, to which only you have access. You are responsible for ensuring appropriate permissions are in place for your files, or departmental files if you are a manager, and that personal data is kept secure, with restricted access and password protected as required.

e. Data Handling

When handling data it is important to follow the Guild's data protection policies and privacy notices. If you are unsure of how you should store data contact the Data Protection Officer, and/or IT department (for electronic data).

f. Mobile devices & removal of data from Guild premises

If you are a user of a Guild/IT Services issued mobile device that holds data it is important to respect the following rules:

- Report any loss of mobile or removable devices immediately to IT Services.
- Do not use mobile devices or removable media as a form of backup. These devices can be unreliable for this purpose.
- Sufficient care must be taken at all times to ensure that the equipment is secure. Where appropriate locking devices or other security measures should be employed.
- You should ensure that any confidential or special data is not kept on mobile or removable devices for longer than is necessary and no longer than stated in the Data Retention Policy.

Data should only be stored and removed from the Guild on an officially issued mobile device or encrypted memory stick. Failure to comply with these guidelines or unauthorised removal of Guild data from Guild premises may result in disciplinary action. Please note that data should not be stored or removed on any personal devices.